

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

An Apple iPhone Cellular Phone, Bearing IMEI
356712087836359, currently located at 9875 Redhill
Drive, Blue Ash Oh 45242, as further described in
Attachment A.

Case No. **1:24-MJ-00503**

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 U.S.C. § 2422(b)
18 U.S.C. §§ 2252(a)(2), (b)(1) & 2252A(a)(2), (b)(1)
18 U.S.C. §§ 2251(a), (e)

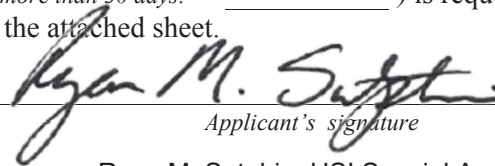
Offense Description

Coercion and enticement of a minor to engage in sexual activity
Receipt and distribution of child pornography
Production of Child Pornography

The application is based on these facts:

Please see attached affidavit.

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

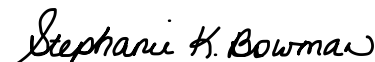
Ryan M. Sutphin, HSI Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
FaceTime video conference (specify reliable electronic means).

Date: **Jun 25, 2024**

City and state: Cincinnati, Ohio



Judge's signature

Stephanie K. Bowman, United States Magistrate Judge

Printed name and title



ATTACHMENT A

The property to be searched is a white Apple iPhone cellular phone bearing IMEI 356712087836359, belonging to Kyle TENNYSON (**SUBJECT DEVICE**). The **SUBJECT DEVICE** is currently located at 9875 Redhill Drive, Blue Ash, OH 45242. This warrant authorizes the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the **SUBJECT DEVICE** described in Attachment A that relate to violations of 18 U.S.C. § 2422(b) (Coercion and Enticement of a Minor to Engage in Sexual Activity), and 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), and 18 U.S.C. §§ 2251(a) and (e) (Production of Child Pornography) which make it a crime to produce child pornography, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;
2. Any images and videos depicting child pornography;
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
4. Any Internet or search history indicative of searching for child pornography or content involving children;
5. Any communications with others in which child exploitation materials and offenses are discussed and/or traded;
6. Any communications with minors, and any identifying information for these minors;
7. Any information related to the use of aliases;
8. Evidence of utilization of cloud storage accounts, email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs;
9. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements;
10. Any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by the devices;
11. Any GPS or geo-location information for the devices or other records reflective of the whereabouts of the device user;
12. Evidence of who used, owned, or controlled the **SUBJECT DEVICE** at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

13. Evidence of software that would allow others to control the **SUBJECT DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
14. Evidence of the lack of such malicious software;
15. Evidence indicating how and when the **SUBJECT DEVICES** were accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the **SUBJECT DEVICES** user;
16. Evidence indicating the **SUBJECT DEVICE** user's knowledge and/or intent as it relates to the crime(s) under investigation;
17. Evidence of the attachment to the **SUBJECT DEVICE** of other storage devices or similar containers for electronic evidence;
18. Evidence of the use of online cloud storage service;
19. Evidence of programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICE**; and
20. Any records or information relating to the presence or use of dark net overlay networks or anonymous proxy networks, such as Tor.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
AN APPLE IPHONE CELLULAR PHONE,
BEARING IMEI 356712087836359,
CURRENTLY LOCATED AT 9875
REDHILL DRIVE, BLUE ASH OH 45242

Case No. **1:24-MJ-00503**

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Ryan Sutphin, being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.
2. I am currently assigned to the Assistant Special Agent in Charge field office in Cincinnati, Ohio. As an agent with the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), I primarily investigate violations of federal criminal laws, including but not limited to, offenses pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251(a) and (e), 2252(a), and 2252A, the interstate transportation of individuals for purposes of prostitution, in violation of 18 U.S.C. § 2421; and sex trafficking of children, or by force, threats of force, fraud, or coercion, in violation of 18 U.S.C. § 1591. Since joining HSI, I have received specific training on human trafficking investigations, child exploitation and child pornography investigations, and I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in multiple forms of media, including computer media. I have also participated in the execution of numerous search warrants involving human trafficking, child exploitation and/or child pornography offenses.
3. The property to be searched is an Apple iPhone cellular phone, bearing IMEI 356712087836359, belonging to Kyle TENNYSON (**SUBJECT DEVICE**).
4. The **SUBJECT DEVICE** is currently held at the Cincinnati offices of HSI, located at 9875 Redhill Drive, Blue Ash, OH 45242, and as more fully described in Attachment A.

5. The applied-for warrant would authorize the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying electronically stored data described in Attachment B.
6. The statements contained in this Affidavit are based on my personal investigation of this matter and on documentation, reports, and other evidence provided by other agents, officers, and investigators involved in the investigation into this matter, including the Cincinnati Police Department (CPD). This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.
7. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime are present within the information located on the **SUBJECT DEVICE**. Specifically, there is probable cause to believe that evidence of violations of the following sections of federal law will be present in the information located on the **SUBJECT DEVICE**:
 - a. 18 U.S.C. § 2422(b), which makes it a crime to use a facility of interstate or foreign commerce to coerce and entice another individual to engage in illegal sexual activities;
 - b. 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1), which make it a crime to distribute and receive child pornography through interstate commerce;
 - c. 18 U.S.C. §§ 2251(a) and (e), which make it a crime to produce child pornography;

PERTINENT FEDERAL CRIMINAL STATUTES

8. It is a violation of 18 U.S.C. § 2422(b) for any person to use the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so.
 - a. For purposes of the statute, 18 U.S.C. § 2427 states that the term “sexual activity for which any person can be charged with a criminal offense” includes the production of child pornography, as defined in section 2256(8).
9. It is a violation of 18 U.S.C. § 2252(a)(2) and (b)(1) for any person to knowingly receive or distribute any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, shipped, or transported in or affecting interstate or foreign commerce or which contains materials which have been mailed or so shipped or transported by any means, including by computer, or to knowingly reproduce any visual depiction for distribution using any means or facility of interstate or foreign commerce or

in or affecting interstate or foreign commerce or through the mails if the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

10. It is a violation of 18 U.S.C. § 2252A(a)(2) and (b)(1) for any person to knowingly receive or distribute – (A) any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and (B) any material that contains child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.
11. It is a violation of 18 U.S.C. §§ 2251(a) and (e) for any person to knowingly employ, use, persuade, induce, entice, or coerce any minor to engage in, or to have a minor assist any other person to engage in, or to transport any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, when he knew or had reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or attempts or conspires to do so.

BACKGROUND INFORMATION

Definitions

12. The following definitions apply to this Affidavit and Attachment B to this Affidavit:
 - a. **“Child Pornography”** includes the definition in Title 18 U.S.C. § 2256(8): any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture whether made or produced by electronic, mechanical or other means, of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.
 - b. **“Visual depictions”** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image (see 18 U.S.C. § 2256(5)).

- c. “**Minor**” means any person under the age of eighteen years (see 18 U.S.C. § 2256(1)).
- d. “**Sexually explicit conduct**” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person (see 18 U.S.C. § 2256(2)).
- e. “**Child erotica**”, as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.
- f. “**Cloud storage**,” as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user’s computer or other local storage device) and is made available to users over a network, typically the Internet.
- g. “**Computer**,” as used herein, refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).
- h. “**Computer hardware**,” as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, “thumb,” “jump,” or “flash” drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).
- i. “**Computer passwords and data security devices**,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- j. “**Encryption**” is the process of converting data into a code in order to prevent unauthorized access to the data.
- k. The “**Internet**” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- l. “**Remote computing service**,” as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.
- m. “**Storage Medium**” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.
- n. “**Tor network**” is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a “circuit.”
- o. “**Internet Service Providers**” or “**ISPs**” are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone-based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite-based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system and can access the Internet by using his or her account name and password.
- p. An “**Internet Protocol address**”, also referred to as an “**IP address**”, is a unique numeric address that computers or electronic devices use to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as “octets,” ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses: static and dynamic. A static

address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

- q. **“Hyperlink”** (often referred to simply as a “link”) refers to a navigation element in a web page or document that automatically brings the referred information (a.k.a. “resource”) to the user when the navigation element is selected by the user. Hyperlinks are part of the foundation of the World Wide Web, but are not limited to a website for HTML.
- r. **“Website”** consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).
- s. **“Uniform Resource Locator”** or **“Universal Resource Locator”** or **“URL”** is the unique address for a file that is accessible on the Internet. For example, a common way to get to a website is to enter the URL of the website’s home page file in the Web browser’s address line. Additionally, any file within that website can be specified with a URL. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.
- t. **“Social Media”** is a term to refer to websites and other Internet-based applications that are designed to allow people to share content quickly, efficiently, and on a real-time basis. Many social media applications allow users to create account profiles that display users’ account names and other personal information, as well as to exchange messages with others. Numerous forms of social media are presently available on the Internet.
- u. A **“wireless telephone”** (or **“mobile telephone”**, or **“cellular telephone”**) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- v. The terms “**records**,” “**documents**,” and “**materials**,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Background on Computers and Child Pornography

- 13. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.
- 14. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera to the computer. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the camcorder to a computer.
- 15. A device known as a modem allows any computer to connect to another computer using telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “Instant Messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.
- 16. The computer’s ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the

last several years. These drives can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital files. One-Terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Media storage devices can easily be concealed and carried on an individual’s person.

17. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer or external media in most cases.
18. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Collectors of Child Pornography

19. Based upon my knowledge, training, and experience in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the collection of child pornography (hereafter “collectors”):
 - a. Collectors may receive sexual stimulation and satisfaction from contact with children, or from having fantasies of children engaged in sexual activity or suggestive poses, or from literature describing such activity.
 - b. Collectors may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Collectors typically use these materials for their own sexual arousal and gratification. Collectors often have companion collections of child erotica. Child erotica are materials or items that are sexually suggestive and arousing

to pedophiles, but which are not in and of themselves obscene or pornographic. Such items may include photographs of clothed children, drawings, sketches, fantasy writings, diaries, pedophilic literature, and sexual aids.

- c. Collectors who also actively seek to engage in sexual activity with children may use these materials to lower the inhibitions of a child they are attempting to seduce, convince the child of the normalcy of such conduct, sexually arouse their selected child partner, or demonstrate how to perform the desired sexual acts.
- d. Collectors almost always possess and maintain their “hard copies” of child pornographic images and reference materials (e.g., mailing and address lists) in a private and secure location. With the growth of the Internet and computers, a large percentage of most collections today are in digital format. Typically, these materials are kept at the collector’s residence, inside the collector’s vehicle, or, at times, on their person, or in cloud-based online storage, to enable easy access and viewing. Collectors usually place high value on their materials because of the difficulty, and legal and social danger, associated with acquiring them. As a result, it is not uncommon for collectors to retain child pornography for long periods of time, even for years.
- e. Collectors often discard child pornography images only while “culling” their collections to improve their overall quality. However, some Collectors have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis. Evidence of this activity, including deleted child pornography, often can be located on these individuals’ computers and digital devices using forensic tools. The very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.
- f. Collectors also may correspond with and/or meet others to share information and materials. They may save correspondence from other child pornography distributors/collectors, including contact information like email addresses, and may conceal such correspondence as they do their sexually explicit material.
- g. Collectors prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
- h. Subscribers to websites that are primarily designed to provide child pornography have a strong likelihood of being collectors of child pornography. This high degree of correlation between subscription and collection behavior has been repeatedly confirmed during several recent nationwide law enforcement initiatives.
- i. Even if collectors use a portable device (such as a mobile phone) to access the internet and child pornography, it is very likely evidence of this activity and access will be found on the **SUBJECT DEVICE** for reasons including the frequency of “backing up” or “synching” mobile phones to computers or other digital devices.

FACTS SUPPORTING PROBABLE CAUSE

20. On April 29, 2024, while working with the Miami Valley Human Trafficking Task Force (MVHTTF), HSI Special Agent Ryan Sutphin, in an undercover (UC) capacity, established a profile on the social media application “Kasual”, an online dating application.
21. On April 30, 2024, at approximately 12:28 a.m. the UC was contacted via direct message by an account identified only as “Man, 33, Dublin”. The suspect would later be identified as Kyle TENNYSON. Initial conversation only lasted a few interactions and stopped at approximately 12:37 a.m. when TENNYSON said “I’m doing alright, just bored haha. How about you?”
22. That same day at approximately 5:21 p.m. Task Force Officer (TFO) Kasey Ballinger resumed the conversation with TENNYSON controlling the undercover account. The UC account sent the message “I’m good... just hanging out”.
23. At approximately 6:17 p.m. TENNYSON messaged the UC, “Can you be honest with me about what your age actually is?” The UC replied, ughhh ok...15”...”everyone stops talking to me tho”...”its not fair...”. TENNYSON replied in part, “It’s just extremely risky to do anything with you sadly :/ I hate the law”. Shortly following that TENNYSON revealed to the UC, “Basically, I was caught for this a few months ago and am currently going through the legal system”...”Girl on bumble said she was 18. She wasn’t. Parents found out. I got screwed.” TENNYSON continued to describe the application making it hard to discuss on the application and offered to text with the UC. The UC agreed asking for TENNYSON’s phone number. TENNYSON said, “Can I ask for one thing first before I do that?”...”Sometimes these things are setups. Could you send me a selfie touching your nose with your pinky finger? Something that ridiculous will help me know you’re real haha”.
24. At approximately 6:56 p.m. the UC sent a selfie style image touching their nose with their index finger. TENNYSON replied, “And I gotta be picky about that pic:p”...”I actually said pinky finger”. TENNYSON added, “There’s a lot of pics with index finger touching nose out there because a lot of people ask for that, so scammers know to find those pics”. At approximately 7:00 p.m., The UC sent a selfie style image depicting their pinky touching their nose. At approximately 7:04 p.m. TENNYSON replied with a similar image, a selfie style photo depicting his pinky touching his nose.
25. At approximately 7:08 p.m. The UC asked, “did you still not want to hang out?”. TENNYSON replied, “Can I ask where exactly you are? I’d want to see how long it would take”. After sending the address the UC asked, “you like younger girls? You said it happened before and u seem ok with me being 15... I like that you’re older...”. TENNYSON acknowledged the UC was portraying a 15-year-old and said he doesn’t seek out younger girls, but once a connection starts to form, it’s hard for him to walk away. TENNYSON added he likes a younger look in girls. The UC asked TENNYSON how long before he would arrive implying they needed to shower. TENNYSON then requested a screenshot of the UC’s location using their phone’s map app, indicating he needed to be

cautious given his current situation. At approximately 7:34 p.m. the UC sent the requested screenshot. TENNYSON requested a second screenshot with a dot indicating the UCs location on the map. At approximately 7:40 p.m., the UC sent the requested image.

26. At 7:43 p.m. TENNYSON stated, the other thing I wanted from you would probably work better anyway". TENNYSON then directed the UC to take a selfie style picture outside showing the hotel sign in the background. The UC sent the requested image at approximately 7:49 p.m. At 7:51 p.m. TENNYSON requested a second pose in the same location. The UC sent the requested image at approximately 7:54 p.m.
27. At approximately 7:59 p.m. the UC said, "ummm what's your name too tho! I'm Carlee". TENNYSON replied "I'm Kyle". The UC asked how far Dublin was and TENNYSON indicated approximately "A little under 2 hours :/". TENNYSON added "I don't mind the trip, but depends how late you go lol". The UC responded saying, "I'm 15 remember?!? I can stay up all night and sleep all day. LOL". TENNYSON continued asking if the UC had their own room and if their parents had a key to it, to which the UC indicated "I have both"...and they are across the hall not right next door too!" TENNYSON replied, "Gotcha, that helps lmao, if there's a lot of noise". The UC later asked, "what exactly do you want to do". TENNYSON replied, asking the UC, "do you finger yourself at all down there"...I'm asking because I wonder if you know how small/large the opening is. I have a dick on the thicker side". The UC continued to imply they were inexperienced sexually and didn't know what to do. TENNYSON later said, "I could give you the experience of what a lover really should do for the girl he's with. It includes all kinds of passionate things, lots of touching, kissing, sucking, all of it :) so one thing couples really like to do is eat on each others private parts. For you of course that's giving a blow job. For me it's eating you out, basically sucking and licking on your clit and all other parts of the pussy".
28. At approximately 8:19 p.m. TENNYSON said, "if you don't mind me asking, do you finger yourself at all down there?"... "I'm asking because I wonder if you know how small/large the opening is." At approximately 8:22 p.m. TENNYSON said, "if you're comfortable enough you can send me a pic spreading it out so I can see how big it is".
29. At approximately 8:31 p.m. TENNYSON said, "When I get there, to be safe, I will let you know I'm there, then I'd like to see you walk out the front door before I come to the door". The UC indicated the stairwell at the side of the building would be better and TENNYSON agreed. TENNYSON indicated he would bring condoms and directed the UC to put three fingers in their vagina to see how it felt. TENNYSON also advised the UC to research different sexual positions if they wanted to, such as "missionary, cowgirl, and doggy".
30. At approximately 11:24 TENNYSON stated he had just parked his vehicle. TENNYSON asked the UC to open the side door to the hotel so he could see her. UC opened the side stairwell door on level 1 and went back inside the hotel. TENNYSON entered the hotel at approximately 11:30 p.m. and was promptly detained by marked officers. The UC later sent a test message to the number they had been communicating with. Officer observed the notification alert when the test message was received by the phone detained from TENNYSON upon arrest.

31. TENNYSON was escorted to a nearby hotel room designated for the operation and advised of his constitutional rights (Miranda warning), which he acknowledged he understood and agreed to answer questions at that time. TENNYSON was carrying a grocery bag at the time of his arrest which contained an open box of 36 count condoms. TENNYSON declined to discuss the specific details about who he planned to meet with at the hotel.
32. As explained above, the **SUBJECT DEVICE** is currently in the lawful possession of HSI, having been initially seized by CPD incident to TENNYSON's arrest. The **SUBJECT DEVICE** was held in an approved CPD property holding facility until it was transferred to HSI custody. Therefore, while HSI might already have all the necessary authority to examine the **SUBJECT DEVICE**, I seek this additional warrant out of an abundance of caution to be certain that an examination of the **SUBJECT DEVICE** will comply with the Fourth Amendment and other applicable laws.
33. The **SUBJECT DEVICE** is currently in storage at the Cincinnati offices of HSI located at 9875 Redhill Drive, Blue Ash, OH 45242. In my training and experience, I know that the **SUBJECT DEVICE** has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the **SUBJECT DEVICE** first came into the possession of law enforcement.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

34. As described above and in Attachment B, this application seeks permission to search the **SUBJECT DEVICE** for evidence in whatever form it is found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the search of the electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B). I submit that, for the **SUBJECT DEVICE**, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:
 - a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.
 - b. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
 - c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a

computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

- d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
35. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the **SUBJECT DEVICE** because:
- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.
 - b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer

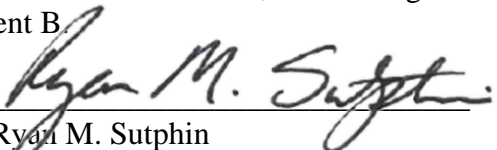
or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence to conceal it from law enforcement).

- c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.
- f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing

the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

CONCLUSION

36. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection to determine whether it is evidence described by the warrant.
37. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items searched. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.
38. Further, because this warrant seeks only permission to examine a device already in law enforcement’s possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.
39. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located on the **SUBJECT DEVICE** described in Attachment A. I respectfully request this Court issue a search warrant for the **SUBJECT DEVICE** described in Attachment A, authorizing the seizure and search of the items described in Attachment B.


Ryan M. Sutphin
Special Agent
Homeland Security Investigations

Sworn and subscribed to before me by reliable electronic means, specifically, FaceTime video conference, pursuant to Fed. R. Crim. P. 4.1, on June 25, 2024.



Hon. Stephanie K. Bowman
United States Magistrate Judge
U.S. District Court for the Southern District of Ohio



ATTACHMENT A

The property to be searched is a white Apple iPhone cellular phone bearing IMEI 356712087836359, belonging to Kyle TENNYSON (**SUBJECT DEVICE**). The **SUBJECT DEVICE** is currently located at 9875 Redhill Drive, Blue Ash, OH 45242. This warrant authorizes the forensic examination of the **SUBJECT DEVICE** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

All records on the **SUBJECT DEVICE** described in Attachment A that relate to violations of 18 U.S.C. § 2422(b) (Coercion and Enticement of a Minor to Engage in Sexual Activity), and 18 U.S.C. §§ 2252(a)(2) and (b)(1) and 2252A(a)(2) and (b)(1) (receipt and distribution of child pornography), and 18 U.S.C. §§ 2251(a) and (e) (Production of Child Pornography) which make it a crime to produce child pornography, including but not limited to the following:

1. Any visual depictions and records related to the possession, receipt, and distribution of child pornography;
2. Any images and videos depicting child pornography;
3. Any and all child erotica, including images and videos of children that are not sexually explicit, drawings, sketches, fantasy writings, diaries, and sexual aids;
4. Any Internet or search history indicative of searching for child pornography or content involving children;
5. Any communications with others in which child exploitation materials and offenses are discussed and/or traded;
6. Any communications with minors, and any identifying information for these minors;
7. Any information related to the use of aliases;
8. Evidence of utilization of cloud storage accounts, email accounts, social media accounts, online chat programs, and peer-to-peer file sharing programs;
9. Evidence of utilization of telephone accounts, Internet Service Providers, and other Electronic Service Providers, including but not limited to monthly statements;
10. Any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by the devices;
11. Any GPS or geo-location information for the devices or other records reflective of the whereabouts of the device user;
12. Evidence of who used, owned, or controlled the **SUBJECT DEVICE** at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

13. Evidence of software that would allow others to control the **SUBJECT DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
14. Evidence of the lack of such malicious software;
15. Evidence indicating how and when the **SUBJECT DEVICES** were accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the **SUBJECT DEVICES** user;
16. Evidence indicating the **SUBJECT DEVICE** user's knowledge and/or intent as it relates to the crime(s) under investigation;
17. Evidence of the attachment to the **SUBJECT DEVICE** of other storage devices or similar containers for electronic evidence;
18. Evidence of the use of online cloud storage service;
19. Evidence of programs (and associated data) that are designed to eliminate data from the **SUBJECT DEVICE**; and
20. Any records or information relating to the presence or use of dark net overlay networks or anonymous proxy networks, such as Tor.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage and any photographic form.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.